EXCEPTION HANDLING IN CELLULAR AUTHENTICATION

TECHNICAL FIELD

[0001] The present application generally relates to exception handling in cellular authentication.

BACKGROUND

[0002] This section illustrates useful background information without admission of any technique described herein representative of the state of the art.

[0003] Cellular networks or more accurately cellular telecommunications networks are ubiquitous in modern societies. To enable a cellular terminal to start communications over a cellular network, the cellular terminals need to attach or register to the network in a network registration process. In the network registration process, a cellular terminal exchanges signals to authenticate itself or more accurately its subscription, typically using a USIM application on a UICC. In the network registration process, the cellular terminal obtains from the network and the SIM access information such as a session key with which the cellular terminal can subsequently communicate in the cellular network. The access information typically changes to prevent re-use of the access information by a possible illegal interceptor.

[0004] Encryption is a basic tool that is employed also in other types of digital cellular systems. Already GSM used encryption to enable mitigating illegal interception. The development of computer technology has subsequently made old encryption techniques more vulnerable, but also helped to enhance the security techniques used in cellular systems. For instance, wide-band CDMA (W-CDMA) was designed for stronger security by enabling also the network to authenticate itself to the cellular terminals. In the W-CDMA, the subscriber identity is provided by a Universal Integrated Circuit Card (UICC) that runs a Universal Subscriber Identity Module (USIM). The USIM produces e.g. a session key based on a shared secret stored on the UICC, challenge and replay attack prevention codes received from the network and cryptographic algorithm that is enhanced over the one used in GSM. Also the authentication signaling is enhanced in the W-CDMA over GSM e.g. for protection against some man-in-the-middle attacks.

[0005] In parallel with the development of security methods for securing the communications in the cellular systems, there are also growing needs for developing the structure of cellular terminals. At present, most cellular terminals contain an identity module slot such as a SIM slot in which a user can place and replace an identity module card such as the UICC. There is also development towards identity modules that are not physically replaceable so as to enable over-the-air change of subscription and/or to prevent theft of the identity module from a cellular terminal. Such software identity modules may be very useful e.g. for built-in vehicular communication systems so that their emergency reporting capabilities and possible burglar control systems could not be easily deactivated by removing an identity module card. While the non-removability of embedded UICCs brings its advantages with respect to theft protection or price, it has also its challenges. One major challenge is the user of the machine that holds the identity module may wish to have another cellular operator. Today, the operator would issue a new card. This is not possible with embedded modules. Therefore, an operator is for the machine use cases not necessarily sure what kind of module will be connected to its network and what capabilities it has. This will lead to error cases that we don't have today and which need to be solved to avoid that the module cannot connect at all.

[0006] While necessary for security, the authentication signaling unfortunately delays completion of network registration procedures. Moreover, the inventors have now identified that in some particular combinations of cellular terminal equipment, network configuration and encryption authentication protocols, a cellular terminal might engage into a perpetually failing loop so that its user could not establish telecommunications connectivity at all.

SUMMARY

[0007] Various aspects of examples of the invention are set out in the claims.

[0008] According to a first example aspect of the present invention, there is provided a method in a cellular terminal, comprising:

[0009] transmitting a request that requires authentication procedure triggering to a cellular network and responsively receiving from the cellular network an authentication request message with an indication of a selected cryptographic algorithm from a group of a plurality of cryptographic algorithms;

[0010] attempting to decode the authentication request message to a decoded authentication request according to the selected cryptographic algorithm and based on a shared secret known by the cellular terminal and a network operator of the cellular terminal;

[0011] producing a determination whether the attempt was successful and the cellular terminal supports the selected cryptographic algorithm in authenticating to the cellular network; and

[0012] in case the determination is positive, based on the decoded authentication request, the shared secret and the selected cryptographic algorithm, producing and encrypting an authentication response message and transmitting the authentication response message to the cellular network; and

[0013] in case the determination is not positive, producing and sending to the cellular network a failure report.

[0014] The request that requires authentication procedure triggering may be a network registration request.

[0015] The request that requires authentication procedure triggering may be a routing area request.

[0016] The request that requires authentication procedure triggering may be a tracking area update request.

[0017] The authentication request may be an authentication request of an evolved packet system architecture.

[0018] The authentication request message may be received from a mobility management entity. The authentication response message may be transmitted to the mobility management entity.

[0019] The cellular terminal may comprise a security entity. The security entity may comprise a secure element and a subscriber identity module application. The cellular terminal may comprise user equipment. The user equipment may be configured to perform communications over radio interface with a base station. The security entity may be configured to decode authentication requests and to produce authentication responses. The user equipment may be selected from a group consisting of: a mobile terminal; a